Patch Release Note

Patch sr264-03 for AT-8600 series switches

Introduction

This patch release note lists the issues addressed and enhancements made in patch sr264-03 for Software Release 2.6.4 on existing models of AT-8600 series switches. Patch file details are listed in Table 1.

Table 1: Patch file details for Patch sr264-03.

Base Software Release File	sr-264.rez
Patch Release Date	30-July-2004
Compressed Patch File Name	sr264-03.paz
Compressed Patch File Size	40912 bytes

This release note should be read in conjunction with the following documents:

- Release Note: Software Release 2.6.4 for AT-8600 Series switches (Document Number C613-10404-00 REV A) available from *www.alliedtelesyn.co.nz/documentation/documentation.html*.
- AT-8600 Series Switch Documentation Set for Software Release 2.6.4 available on the Documentation and Tools CD-ROM packaged with your switch, or from *www.alliedtelesyn.co.nz/documentation/documentation.html*.

WARNING: Using a patch for a different model or software release may cause unpredictable results, including disruption to the network. Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesyn International. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesyn International can not accept any type of liability for errors in, or omissions arising from the use of this information.

Some of the issues addressed in this Release Note include a level number. This number reflects the importance of the issue that has been resolved. The levels are:

Level 1 This issue will cause significant interruption to network services, and there is no work-around.

Level 2 This issue will cause interruption to network service, however there is a work-around.

Level 3 This issue will seldom appear, and will cause minor inconvenience.

Level 4 This issue represents a cosmetic change and does not affect network operation.

Features in sr264-03

Patch sr264-03 includes all issues resolved and enhancements released in previous patches for Software Release 2.6.4, and the following enhancements:

PCR: 31225 Module: IPG Level: 3

While the switch was set with a CIDR interface address, when it received an ECHO request with a network broadcast destination address for a class C network, the switch sent the ECHO reply packet. Also, the switch forwarded the ECHO request packet using a broadcast MAC address. These issues have been resolved.

PCR: 40355 Module: VRRP Level: 2

When an IP interface is in a down state and VRRP is configured on the interface, VRRP should be disabled. If it was enabled, VRRP could transition to "INITIAL" state. This issue has been resolved.

PCR: 40357 Module: SW56 Level: 2

The **L3 filter nomatchaction** parameter was not applied for some IP traffic on the switch. This issue has been resolved.

PCR: 40405 Module: ENCO Level: 2

If the ENCO process used to encrypt an ISAKMP packet failed, a switch reboot could occur. This issue has been resolved.

PCR: 40415 Module: VRRP Level: 2

When a master VRRP router was configured from a boot script, the transition to the MASTER state occurred before the Layer 2 interface had been initialised, preventing the gratuitous ARP from being sent. This issue has been resolved.

PCR: 40417 Module: OSPF Level: 3

When LS Acks (Link State Advert acks) were received, they were compared against the transmitted LSA (Link State Advert). If it was the same, the LSA was removed from the re-transmission list. The algorithm used in this check has been changed to be compliant with the algorithm specified in section 13.1 of RFC2328, to determine if the LS Ack received is the instance as the LSA.

PCR: 40440 Module: CLASSIFIER Level: 3

For those classifiers that specified the IP protocol as a match criterion, the IP protocol number was being stored and displayed in a configuration file as a hexadecimal value rather than a decimal value. This issue has been resolved.

PCR: 40441 Module: IPG, VRRP Level: 4

If VRRP was enabled and a **reset ip** command was issued followed by a **disable vrrp** command, then the device would still reply to pings, even though the device was no longer the VRRP master. Duplicate echo replies were seen on the device sending the pings. This issue has been resolved.

PCR: 40446 Module: DHCP Level: 2

In certain situations, if a DHCP client used a DHCP relay agent to request IP addresses from the switch acting as the DHCP server on a different subnet, it was not be able to renew the IP address allocated to it. This issue has been resolved.

PCR: 40447 Module: CORE, SWI, SW56

Support was added for new fibre uplink modules A45SC, A45SCSM, and GBIC uplink module A47.

PCR: 40453 Module: IPG Level: 2

Particular IP packets (unicast destination IP, but multicast destination MAC) could result in a memory leak, which in some cases could cause the device to stop responding to the command line. This issue has been resolved.

Features in sr264-02

Patch file details are listed in Table 2.

Table 2: Patch file details for Patch sr264-02.

Base Software Release File	sr-264.rez
Patch Release Date	06-July-2004
Compressed Patch File Name	sr264-02.paz
Compressed Patch File Size	9288 bytes

Patch sr264-02 includes the following resolved issues and enhancements:

PCR: 40360 Module: SWITCH Level: 3

Factory LED tests (**enable/disable switch led** test for AT-8800 series switches only and **enable/disable switch stpf**) were removed prior to release 2.6.4. This issue has been resolved.

PCR: 40374 Module: PORTAUTH, USER, UTILITY

Support has been added for EAP types TLS, TTLS, and PEAP when the switch is acting as an 802.1x authenticator. See "The Authentication Server" on page 5 for more information.

PCR: 40414 Module: TM, CORE Level: 3

Factory Autoburn test caused a switch reboot when BIST started to run. This issue has been resolved.

The Authentication Server

The authentication server verifies the supplicant's details, passed to it by the authenticator. This implementation of 802.1x control requires that a port acting as an authenticator must communicate with a RADIUS authentication server. The RADIUS server must be capable of receiving and deciphering EAP in RADIUS packets.

The authentication server must be connected to a port on the switch which does not have port authentication enabled, or is set with CONTROL=AUTHORISED.

The supported supplicant encryption mechanisms for communication with the RADIUS server are EAP-MD5 and EAP-OTP. With this enhancement the encryption methods supported by authenticators are EAP-MD5, EAP-OTP, EAP-TLS, EAP-TTLS, and EAP-PEAP.

Steps in the Authentication Process

Until authentication is successful, the supplicant can only access the authenticator to perform authentication message exchanges, or access services not controlled by the authenticator's controlled port.

Initial 802.1x control begins with an unauthenticated supplicant and an authenticator. A port under 802.1x control acting as an authenticator is in an unauthorised state until authentication is successful.

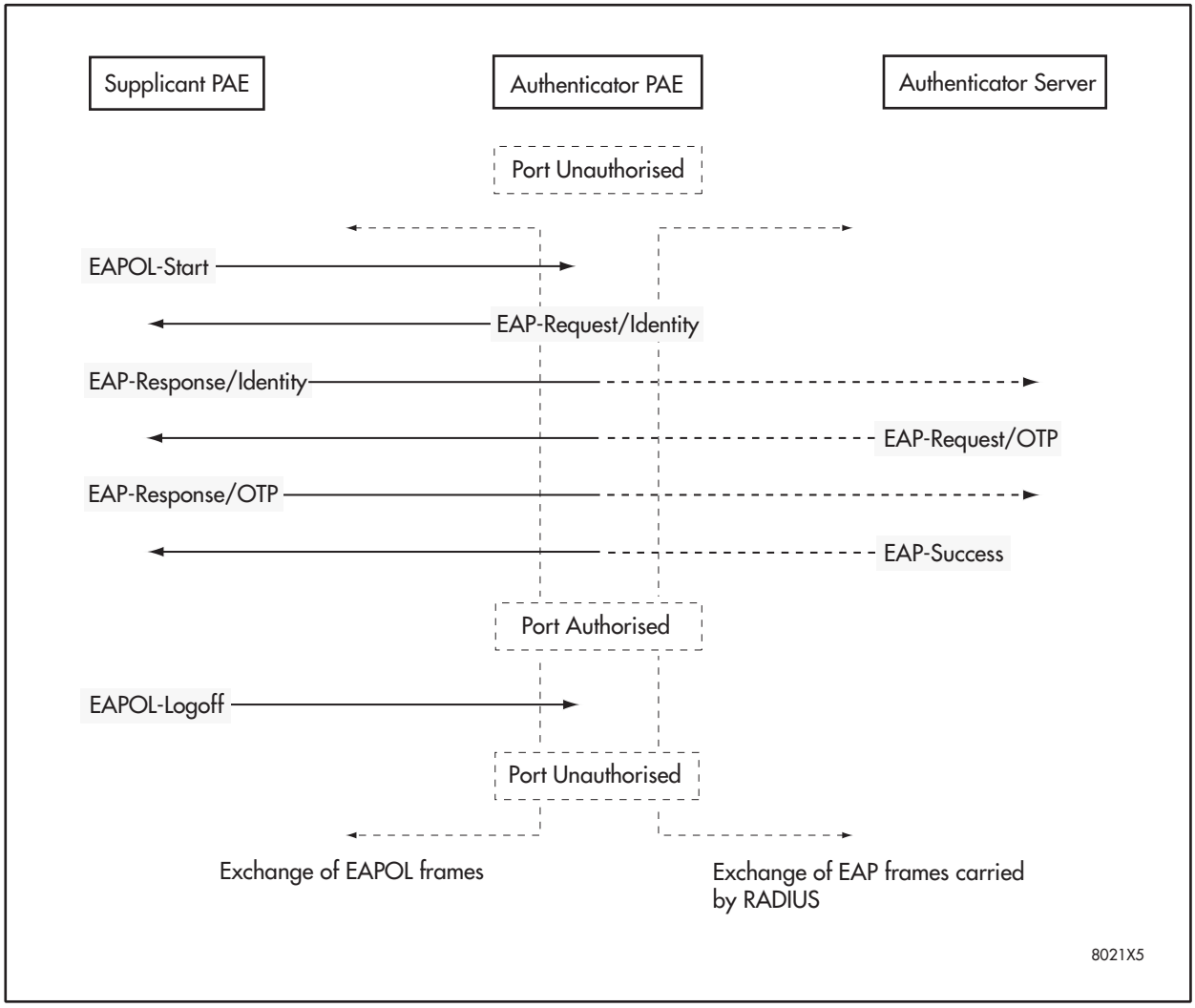
1. Either the authenticator or the supplicant can initiate an authentication message exchange. The authenticator initiates the authentication message exchange by sending an EAPOL packet containing an encapsulated EAP-Request/Identity packet. The supplicant initiates an authentication message exchange by sending an EAPOL-Start packet, to which the authenticator responds by sending an EAPOL packet containing an encapsulated EAP-Request/Identity packet.
2. The supplicant sends an EAPOL packet containing an encapsulated EAP-Response/Identity packet to the authentication server via the authenticator, confirming its identity.
3. The authentication server selects an EAP authentication algorithm to verify the supplicant's identity, and sends an EAP-Request packet to the supplicant via the authenticator.
4. The supplicant provides its authentication credentials to the authenticator server via an EAP-Response packet.
5. The authentication server either sends an EAP-Success packet or EAP-Reject packet to the supplicant via the authenticator.
6. Upon successful authorisation of the supplicant by the authenticator server, a port under 802.1x control is in an authorised state, unless the MAC associated with the port is either physically or administratively inoperable. Also upon successful authorisation of the supplicant by the authenticator server, the supplicant is allowed full access to services offered via the controlled port. If piggybacking is enabled on the authorised authenticator port, any other device connected will also be give full access.

7. When the supplicant sends an EAPOL-Logoff message to the authenticator the port under 802.1x control is set to unauthorised.

A successful authentication message exchange, initiated and ended by a supplicant using OTP authentication, is shown in below.

To minimise the risk of denial-of-service attacks by issuing EAPOL-Logoff messages to an Authenticator Port Access Entity (PAE) from a third party device, we recommend that 802.1x not be used in a shared media LAN.

Figure 1: Authentication Messaging Exchange Initiated by the Supplicant.



Availability

Patches can be downloaded from the Software Updates area of the Allied Telesyn web site at *www.alliedtelesyn.co.nz/support/updates/patches.html*. A licence or password is not required to use a patch.